Software Engineering Institute

Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase I

Greg Porter

November 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-020

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by the Department of Homeland Security (DHS) Federal Network Resilience (FNR) division under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0000682

Table of Contents

List of Tables

Acknowledgments

This work was funded by a grant from the United States Department of Homeland Security (DHS) Federal Network Resilience (FNR) division. Additionally, the authors express our gratitude to the anonymous cybersecurity experts from cloud service providers who generously shared their insights and their time. Their contributions helped us better understand the controls that cloud service providers have deployed to manage insider risks as well as their concerns about their insider threat management competencies. We give a special thanks to our team member and SEI professional editor Paul Ruggiero for improvements to the report.

Abstract

In early 2013, researchers in the CERT® Insider Threat Center contacted commercial and government cloud service providers (CSPs) about participating in research to gain a preliminary understanding of implemented administrative and technical controls that they are using to identify and manage the threats posed by insiders. These CSP participants provided frank and meaningful insight about their insider threat management programs and enterprise security practices. This report contains the observations obtained from interviewing the CSP personnel who volunteered to participate as well as an analysis of CSP management of insider threat based on the information obtained in interviews, observations of implemented insider threat controls, and risk considerations.

1 Introduction

For many businesses and consumers that use them, cloud service providers (CSPs) are counted on, often implicitly, to provide a service that is convenient, reliable, and secure. However, in the absence of specific service level agreements, it can be difficult for customers to ascertain how their data are being protected at rest, in process, and in transit at multiple levels of the stack as it traverses a CSP's infrastructure.

CSPs should carefully select and monitor the personnel who have access to customer and internal resources, up to and including sensitive data such as intellectual property and personally identifiable information (PII). Customers' systems that rely solely on the CSP for security could be at risk of damage to the confidentiality, integrity, and availability of those resources and data. A CSP must not only have well-governed security controls to service its clientele, but also appropriate administrative, physical, and technical safeguards to monitor and manage its employees, contractors, and partners, as well as to identify potential indicators of insider threat activity.

The CERT® Insider Threat Center defines a *malicious insider* as a "current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" [Cappelli 2012].

According to Verizon's *2013 Data Breach Investigations Report* [Verizon 2013], which is the compiled analysis of more than 47,000 security incidents and 621 confirmed data breaches, 14% of the breaches investigated were perpetrated by insiders. Similarly, the Ponemon Institute's *2012 Cost of Cyber Crime Study: United States* research report [Ponemon 2012] indicates that 38% of its 56 participating companies were victims of malicious insider cybercrime. Acts perpetrated by malicious insiders resulted in an average cost of $166,251 per incident and, of the cyber crimes noted, took the longest to resolve, averaging 57.1 days.

Malicious insiders are also recognized as a top security consideration when choosing a CSP [Mello 2013]. While still an emerging area of incident analysis, threats and subsequent breaches that occur in a CSP due to insiders represent risks that must be appropriately accounted for as organizations evaluate CSP options.

Depending on contractual arrangements and deployed controls, a customer likely has extremely limited visibility into the internal security processes and countermeasures that the CSP relies on to adequately protect its data and systems. If those controls are governed inadequately, authorized internal CSP personnel could compromise the CSP and its customers.

Against this backdrop, the United States Department of Homeland Security (DHS) Federal Network Resilience (FNR) division tasked the CERT Division of the Software Engineering

® CERT® is a registered mark owned by Carnegie Mellon University.

Institute (SEI) at Carnegie Mellon University to obtain a preliminary understanding of implemented administrative and technical controls that CSPs may be using to identify and manage the threats posed by insiders.

This report contains the following elements we derived from this research project:

- preliminary analysis obtained through interviews with five participating CSPs (In our analysis, we took the insights of the interview respondents as fact about the CSPs.)
- observations of controls, categorized as either administrative (i.e., process or organization specific) or technical safeguards, that participating CSPs implemented to manage insider behaviors
- risk considerations that may assist CSPs as they develop, implement, monitor, and audit insider threat management processes

1.1 Summary of Key Findings

The priority of organizations in the rapidly expanding CSP sector has been to establish a market presence by acquiring customers and managing subsequent growth. As growth outpaces development of internal and sector-wide processes and practices, even large CSPs have become relatively immature organizations, specifically with respect to focusing on and prioritizing the insider threat vector.

Underlying business processes and administrative controls that can and should govern effective detection and mitigation of insider activities appear to be generally unstructured. Other notable observations of our preliminary research include the following:

- No CSP's risk assessment practices explicitly address insiders as a potential threat.
- No respondents include insider threat as part of their security awareness and training programs.
- Only 60% of CSPs have a mobile-device-management program in place, such as remote wiping and requiring a passcode, that covers all employees. This deficiency can create significant opportunities for data exfiltration, by insiders and otherwise.
- There does not appear to be well-defined processes established among Human Resources (HR), Legal, and Information Security personnel regarding suspicious insider behaviors and procedures that should be followed once a reasonable indicator is obtained.
- Only 40% of respondents use hardened server images for their cloud infrastructure or their corporate servers.
- Encryption, if used, does not appear to be used uniformly.
- All CSPs require multifactor authentication for remote access.
- As an insider threat mitigation strategy, all CSPs employ some form of Security Information and Event Management (SIEM) technology; however, such technologies do not appear to be well tuned for insider threat detection.

2 Methodology

In the first quarter of 2013, we contacted both commercial and government CSPs about participating in the research project. The observations in this report were obtained from interviewing CSP personnel, whose roles ranged from security analysts and chief/senior security architects to vice presidents of information security and directors of technical services. These respondents provided frank and meaningful insight to us regarding their insider threat management programs and enterprise security practices.

We used the information respondents shared in the interviews to describe a current state of the practice regarding the insider threat and CSPs. We categorized the feedback using the following criteria:

- administrative controls—the CSP's nontechnical measures, such as operational policies, organization structures, procedures, standards, and guidelines, that can be used to support insider threat management processes
- technical controls—the technologies the CSP uses to manage, monitor, and protect both customer and internal data and systems from insider threat activities, including technical safeguards such as access and audit controls, data encryption and key management, and mobile device management

We also asked respondents how their CSP would manage various insider threat scenarios beyond implementing specific controls. The scenarios included

- employees abusing their authorized privileges and/or accessing nonauthorized resources
- employees using their cloud infrastructure access to initiate attacks against other organizations
- customers using their access to hosted applications and/or the infrastructure to compromise the CSP or other targets of interest

Lastly, respondents shared with us their general operational insights regarding their processes for network monitoring, security awareness, incident response, and mobile device management, as well as relationship dynamics among functional business units such as HR, Legal, and Information Security departments. Where practical, we included noteworthy observations of these areas in our analysis.

3 Cloud Service Provider Models

As part of this preliminary analysis, we recruited participants from each of the CSP models described in this section, including commercial CSPs as well as those authorized via the Federal Risk and Authorization Management Program (FedRAMP) [GSA 2013].

The National Institute of Standards and Technology (NIST) Special Publication 800-145 (NIST SP 800-145) defines three types of cloud services: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [Mell 2011]. The balance of control between the CSP and the customer varies among these three models. NIST SP 800-145 describes the three service models as follows:

> *SaaS—The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*
>
> *PaaS—The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*
>
> *IaaS—The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).* [Mell 2011]

4 Preliminary Observations

Based on a limited number of respondents, we categorized the information provided as observations of either an administrative or technical practice. Though this analysis in no way represents an exhaustive audit, because all observations were obtained through limited interview sessions, it did reveal key control areas that provide initial insights into current insider threat practices among a representative sampling of CSPs.

4.1 Administrative Controls

In this analysis, administrative controls represent the CSP's nontechnical measures that can be used to support, either directly or indirectly, insider threat management processes. These controls include operational policies and organizational structures, procedures, standards, and guidelines. The following subsections describe our preliminary observations.

4.1.1 Enterprise Security Governance Models

Respondents indicated that enterprise security governance programs, and the models used to define and support them, varied among CSPs. Of participating CSPs, 20% delved significantly into recognized control catalogs such as NIST SP 800-53 [NIST 2009] and the Cloud Security Alliance Cloud Controls Matrix [CSA 2013] (CCM), while 20% obtained formal ISO/IEC 27001:2005 [ISO/IEC 2005] certification of the Information Security Management System (ISMS) governing their cloud operations. One respondent indicated that his CSP was using ISO/IEC 27002:2005[1] to build conformant information security practices, while recording evidentiary support of that conformance for certifying its ISMS in the future.

An interesting nuance between the commercial and government CSPs that contributed to this review is the information security codes of practice they opt to use. Some CSPs are required to adhere to specific requirements, such as those detailed in FedRAMP processes in the government sector. Those in the commercial sector tend to rely more heavily on the ISO/IEC 27000 family of standards for control guidance.

Although the codes of practice are not mutually exclusive and account for the flexibility to appropriately integrate controls from other security frameworks, there did appear to be a degree of rigidity in adhering to certain models. Those in the commercial sector were only vaguely familiar with the FedRAMP program, while those in the government sector appeared to acknowledge the ISO/IEC standards primarily by name alone. Although respondents mentioned and had used the CCM, it did not appear to have been implemented as robustly as the other models.

None of the previously mentioned control models explicitly defines an insider threat control area. Rather, they all advocate the use of risk assessments to select additional security controls to

[1] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *ISO/IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management. ISO, 2005.*

address particular organizational needs based on tolerances for risk, such as those that insider threats may introduce and pose over time.

A potential caveat regarding the use of such models is their prescriptive nature. An organization might unintentionally overlook controls not documented in the framework. This tendency could partially explain why some CSPs may lack a formal insider threat management program; it's not expressly presented in commonly used information security codes of practice. That stated, the CERT Division has mapped best practices such as those outlined in NIST 800-53 and ISO/IEC 27002 to insider threat best practices in the *Common Sense Guide to Mitigating Insider Threats, 4th Edition* [Silowash 2012], which was published by the SEI in 2012.

4.1.2 Insider Threat Program Formalization

Of the CSPs that participated in this analysis, no respondent reported a formal program specifically developed to address insider threat. This shortcoming does not suggest that the CSPs were unaware of insider risks, but rather that processes designed to recognize and manage insider threats appear to be ad hoc and not fully institutionalized in terms of process implementation. As previously mentioned, this situation may be somewhat attributable to the information security governance models used by the CSPs or the lack of resources assigned to address growth.

All respondents indicated that their CSP documented and implemented risk assessment practices; however, the CSPs did not appear to target enterprise risk assessments focused on insiders as a potential threat to the confidentiality, integrity, and availability of the CSPs' (as well as their customers') mission-critical information. This oversight may also indicate that none of the CSPs was willing to share even high-level information regarding insider incidents where the confidentiality, integrity, and availability of mission-critical assets were in imminent danger of being compromised.

Lastly, while the CSPs were familiar with the SEI's CERT Division, they were less familiar with the CERT Insider Threat Center and the research and analysis its researchers have done to combat insider cyber threats. The interaction between the CERT Division and the CSP in this analysis provided a unique opportunity to convey current best practices (e.g., those detailed in the *Common Sense Guide to Mitigating Insider Threats, 4th Edition* [Silowash 2012]).

4.1.3 Security Awareness and Training

None of the participating CSPs included insider threat as part of their security awareness and training program. To some extent, the security awareness and training programs implemented by a few CSPs appear to lack commonly expected functionality, such as

- an automated, web-based delivery mechanism
- a way to track employee training efforts, including when employees complete particular training modules and/or requirements
- follow-up testing to determine comprehension of information on security-related concepts

Although not precisely addressing insider threats, one CSP used internal security conferences to engage employees with a range of relevant information security issues and to raise general security awareness. The conferences provide a forum for CSP employees to ask security personnel questions about security-related issues, polices, and procedures, providing two-way

communication and a useful feedback mechanism for the organization. They bring in external security-related vendors occasionally to speak as well. This approach to security awareness and training provides an excellent opportunity to introduce insider threat concepts and research, among other security areas.

Respondents from a contributing CSP mentioned that their chief information security officer (CISO) had not yet "bought into the [notion of] insider threat [management]" as an area that merits specific attention. This comment speaks directly to the need for enhanced security awareness and training regarding insider threats. Ideally, organizations should offer training that exposes the threats that insiders present to each area of the CSP's operations, from executive leadership and the board of directors to middle management and support personnel.

Lastly, at least one respondent mentioned that her customer base historically has not asked about how the CSP manages insider threat. Compromised networks are often the direct result of well-intentioned employees not fully understanding prevailing threats, both from insiders and otherwise, so the deployment of effective, validated security awareness training cannot be understated.

4.1.4 Human Resources

All respondents indicated that their CSPs require background checks for all newly hired employees and contractors. They may also perform criminal and financial background checks, depending on the classification of the information to be accessed and the perceived risks.

The CSPs did not appear to have established formal, well-defined processes among HR, Legal, and Information Security personnel (or other personnel) regarding suspicious insider behaviors and procedures that should be followed once an indicator is obtained. In many instances, CSP middle managers must identify disgruntled employees and notify HR personnel, who may then initiate further intervention, such as contacting the Legal department, requesting additional employee monitoring, counseling the employee, or terminating the employee.

In instances where insider activity is suspected, CSPs can and do use SIEM technologies to support the continuous monitoring of employee actions, using these data to better understand insiders' system-level activities. Only one respondent mentioned an instance in which a SIEM system was used to assist the confirmation of an employee's concerning behavior. The employee was terminated, in part, based on supporting data provided by the company's SIEM platform.

Insider threat training for HR or other personnel as part of the CSPs' cybersecurity awareness programs does not appear to currently exist. Several respondents indicated that they have "been lucky" thus far to avoid a significant insider event.

4.1.5 Mobile Device Management

Mobile devices introduce new security threats and challenges to organizations, including CSPs. Respondents for each CSP contributing to this analysis mentioned that their CSPs support a hybrid approach that permits both enterprise-issued and employee-owned devices in the organization. Employee devices were generally limited only to email access. For the most part, company-issued laptops have full-disk encryption for CSPs that use them; however, at least one respondent stated that, at present, only a fraction of her CSP's laptops are encrypted. Of all the

respondents, 20% have not considered the overall "data at rest" issue where policy, practices, and enabling tools can help to address digital asset risks.

Apple iOS and the Android operating system appear to be the primary mobile platforms on enterprise and employee mobile devices; Windows Mobile OS and Blackberry 10 are used far less.

From a threat management perspective, 60% of the respondents questioned indicated that their CSPs require mobile devices to use passcodes as an initial security control and that CSPs can remotely wipe devices if needed. The other 40% either did not have mobile-device-management controls in place or had them in place only for a subset of employees. Some respondents pointed to their Acceptable Use Policy as providing general control over mobile devices. Many respondents' CSPs appear to be developing policies or procedures regarding mobile device hardening and application deployment. These policies and procedures are designed to prevent employees from using their mobile device to record internal conversations, take photos and/or videos of operations, bypass encryption, or use on-board storage. Most (60%) of the respondents' CSPs also are using mobile device management (MDM) software to provide additional visibility into their mobile deployment.

Even though these administrative and technical challenges are similar to other industries still coming to terms with mobile devices, a lack of MDM platforms, device hardening, and on-board antimalware detection could subject CSPs to data exfiltration opportunities, from insiders and otherwise, as well as malicious code entry into the network from a mobile endpoint.

4.1.6 Hardware and Software Hardening

Unnecessary accounts, enabled ports, services that serve no business justification, and poorly patched systems provide entrances for insiders and external threat sources alike to compromise CSP infrastructures and data.

Of all respondents, 40% mentioned the use of standardized, hardened images regarding the underlying operating systems and applications used in their cloud-based and corporate (e.g., business) network environments. CSPs perform quality assurance testing to validate the appropriate configurations prior to production implementation and to control and monitor access and updates to their image libraries in an effort to prevent internal employees from unauthorized access and modification of such images. Conversely, a similar degree of control does not appear to be extended to commonly used mobile devices, such as employee- and corporate-owned phones and tablets.

One respondent mentioned that while his CSP hardens internal hardware and software infrastructure assets, it does not perform any such actions for its customers; the onus of doing so is entirely on the client. He stated that the CSP can assist a customer with hardening its cloud-based services for an additional fee, but that most customers opt out of such services.

4.2 Technical Controls

Technical controls are the technologies the CSP uses to manage, monitor, audit, and protect customer and internal data and systems from malicious activities by insiders and external sources. We discussed technical safeguards as part of the interview process, including the following:

- security monitoring
- data encryption and key management
- access and audit controls (especially of the control plane as well as the data and service planes)

4.2.1 Security Monitoring

The volume of CSP customers, coupled with the knowledge and access of insiders, must be met with a proportionate amount of monitoring to maintain situational awareness of cloud infrastructures and potentially malicious activity. While a definitive understanding of the monitoring technologies, process, and metrics a CSP employs is beyond the scope of this analysis, we attempted to gain basic insights into how CSPs monitor their environments.

All respondents indicated that their CSPs use a centralized log collection repository, correlation, and analysis engine to assist with common infrastructure challenges ranging from flow analysis and network baselining to intrusion detection and the identification of suspicious employee behaviors. The use of such an engine is encouraging, since organizations with SIEM solutions in place experienced a substantially lower cost of recovery, detection, and containment than organizations that did not.

When we asked respondents about specific signatures that were useful for detecting suspicious insider activities, none were mentioned. Instead, the CSPs appeared to rely primarily on the default rule sets made available through the technology used, such as a SIEM system. Although respondents indicated that their CSPs do customize network monitoring rules for detecting events, such as newly introduced malicious code, some mentioned that default SIEM signatures for detecting insider cyber activities were too basic and lacked appropriate feedback "in plain English" as to what a reasonable signature should entail.

One respondent mentioned her CSP's use of a SIEM system, but that signatures specific to insider activities were the "next step" in the rollout. We mentioned the CERT Division's *Insider Threat Control: Using a SIEM Signature to Detect Potential Precursors to IT Sabotage* as a useful reference during discussions with respondents [CERT Insider Threat Center 2011]. A preliminary indication is that additional awareness and training for CSP personnel may be needed in this area.

Another respondent stated that his CSP used monitoring techniques to identify internal employees engaging in unauthorized behaviors, such as conducting TCP/IP port scans against the production network. In this instance, the CSP used its SIEM software to initially identify the activity and alert the CSP's information security analyst. The actor was then informed of her noncompliant behavior and placed on an internal watch list to monitor for repeat offenses. This particular instance did not result in termination, but it reinforced the documented policy that employee actions can and will be monitored.

Respondents pointed out that their CSPs monitor their control planes and the resources that network engineers and related staff may be accessing. Some respondents mentioned that beyond providing availability and the requisite hardware or software, their CSPs have little visibility into their customer environments, which can be an intentional requirement of the service agreement. One respondent mentioned that her CSP can provide enhanced monitoring (e.g., intrusion detection and prevention) for the customer, but only if requested.

When asking what common monitoring metrics respondents deemed important, we included the following:

- internal malware infections
- server compromises
- workstation compromises
- changes to critical systems
- account brute-force attempts
- geolocation attack origination

One respondent mentioned that he would like to see a metric of the overall status of "employee happiness" based in some way on individual end users' network activities, such as sites visited, hours of access, and software installed. The organization might use these metrics to establish a baseline or common indicators of employees' (cyber work) "health" in relation to their network activity.

In terms of network dynamics, one respondent likened her corporate culture and resultant network to that of a large university. She indicated that though detective, preventive, and corrective controls are in place, it can be difficult to find a balance between security and productivity; the CSP does not want monitoring and auditing to restrain creativity and information sharing.

The respondent also mentioned the challenges of attempting to proactively manage ongoing virtual machine proliferation once it has begun. Such instances could make establishing a network or end-user baseline difficult because there is no normal baseline from which to validate deviations. Arguably, the absence of a baseline makes suspicious insider events very difficult to identify. This level of control appears to be in stark contrast to the cloud services the CSP provides to its customers, which the respondent mentioned were more controlled and monitored than its internal corporate network.

Using SIEM technology permits a CSP to continuously monitor employee actions and identify potentially harmful insider events. Combining SIEM technology with other monitoring techniques has the most potential for creating frameworks for insider threat discovery. However, it will be a long path to maturity. Knowing which indicators indicate malicious insider behaviors is useful to the CSP participants in this analysis; they would benefit from additional guidance in this area.

4.2.2 Data Encryption and Key Management

Each respondent mentioned the use of encryption for data at rest and in transit. One CSP encrypts all customer files in flight using Triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES), depending on the browser, and uses AES encryption for data at rest. Customer files are stored in an encrypted partition; each file is encrypted with a unique key that is not stored on the customer server. All internal data storage areas are encrypted, regardless of the actual data type; the CSP's cryptographic module (which implements encryption, decryption, message authentication, and/or hash digest functionality using hardware, software, and/or firmware) meets the overall requirements applicable to Level 1 security of Federal Information Processing Standard (FIPS) 140-2 [NIST 2013]. (File encryption is a core component of this particular CSP's business model.)

Other CSPs encrypt internally used, “high-risk” laptops, such as those belonging to executives, network engineers, traveling sales personnel, and remote workers. These users are generally discouraged from placing sensitive data on mobile devices. One respondent indicated that some internal areas of his CSP’s network “have encryption and some do not” but chose not to elaborate.

Most respondents seemed to agree that it is the customer’s responsibility to encrypt files and containers and that making such decisions on behalf of the customer is often beyond the typical scope of services. Regarding internal operations, CSPs seem to be largely driven by regulatory requirements, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and various state breach acts regarding what information must be encrypted and what does not, as well as who has access to it. To thwart the loss of sensitive internal information, some respondents mentioned the use of data loss prevention (DLP) appliances as well as the ability to engage a Transport Layer Security (TLS) proxy to inspect encrypted TLS traffic.

One respondent whose CSP does not offer data-at-rest encryption services did not know if there was a policy to “zero out” raw disk blocks of internet small computer system interface (iSCSI) targets before they were given back to the disk pool after being used by a customer. The respondent indicated that it “may” be solely the customer’s responsibility to ensure that DLP practices are addressed. Obviously, this oversight could provide the insider a simple mechanism for discovery and exfiltration of data from the CSP’s customer as well as the CSP itself.

Internal management of encryption keys is an area that warrants further analysis regarding the use of CSP encryption. Questions such as the following exceeded the scope of this analysis, yet they are tantamount to understanding insider risks concerning who ultimately controls and accesses protected information in the CSP:

- How are keys stored?
- Who has access to them?
- From where can they be accessed?

If encryption keys are compromised by an insider, private customer and internal CSP data could enter the public domain in short order.

4.2.3 Access and Audit Controls

CSP participants seemed to use multifactor authentication for remote access to their corporate networks and control infrastructures. Traditional user name and password authentication is used to validate end users working locally. At least one CSP uses strong authentication for providing employee access to key internal resources, such as control plane access needed by network engineers to support virtualized customer services. The respondent representing this particular CSP indicated that the provider limits the use of administrative accounts on its internal network and monitors resources and staff for anomalous behavior.

All respondents indicated that their CSPs implemented appropriate policies, procedures, and workflows to govern account provisioning and deactivation (e.g., minimizing the number of personnel who have administrative privileges, using only the administrative accounts when required, and using focused auditing and monitoring where administrative or privileged functions are used).

5 Additional Considerations

Preliminary analysis regarding the state of insider threat management practices in CSPs indicates that the providers, as well as the customers they support, can benefit from deployed administrative, physical, and technical controls, and these controls can improve the ability of CSPs to detect, monitor, and manage insider-related attacks. The considerations in the following sections may help CSPs gain better insight into insider threat preparedness.

5.1.1 Insider Threat Diagnostic Assessment

A simple yet effective means for gaining an initial understanding of capability is to conduct a diagnostic assessment of existing practices against the *Common Sense Guide to Prevention and Detection of Insider Threats, 4th Edition* [Silowash 2012]. By doing so, organizations can efficiently identify gaps, develop specific recommendations and mitigation strategies that address observed deficiencies, and secure a comprehensive view of insider strengths and weaknesses.

Insider threat management practices can be categorized into the three types illustrated in Table 1.

Table 1: Three Types of Insider Threat Management Practices

Practice Type	Description
Fully Implemented	Sufficient administrative, physical, or technical controls exist to satisfy the assessed practice.
Partially Implemented	An existing administrative, physical, or technical control was identified that would partially satisfy the requirements of the assessed practice. However, additional actions must be taken to fully satisfy the requirements.
Absent	No existing administrative, physical, or technical control was observed that would fully satisfy the intent of the assessed practice.

Table 2 presents a worksheet that CSPs can use to conduct a diagnostic assessment of their practices against the insider threat management practices in the *Common Sense Guide to Prevention and Detection of Insider Threats, 4th Edition* [Silowash 2012].

Table 2: Insider Threat Management Practices Worksheet

Practice	Fully Implemented	Partially Implemented	Absent
Practice 1: Consider threats from insiders and business partners in enterprise-wide risk assessments.			
Practice 2: Clearly document and consistently enforce policies and controls.			
Practice 3: Incorporate insider threat awareness into periodic security training for all employees.			
Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.			
Practice 5: Anticipate and manage negative issues in the work environment.			
Practice 6: Know your assets.			
Practice 7: Implement strict password and account management policies and practices.			
Practice 8: Enforce separation of duties and least privilege.			
Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.			
Practice 10: Institute stringent access controls and monitoring policies on privileged users.			
Practice 11: Institutionalize system change controls.			
Practice 12: Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.			
Practice 13: Monitor and control remote access from all end points, including mobile devices.			
Practice 14: Develop a comprehensive employee termination procedure.			
Practice 15: Implement secure backup and recovery processes.			
Practice 16: Develop a formalized insider threat program.			
Practice 17: Establish a baseline of normal network device behavior.			
Practice 18: Be especially vigilant regarding social media.			
Practice 19: Close the doors to unauthorized data exfiltration.			

5.1.2 Proactive Project/Employee Engagement Scoring

CSPs may be able to proactively identify precursors of suspicious insider behaviors by combining internal network-related event information, social media data, and employee behavioral characteristics obtained via feedback from project managers and supervisors. Assuming that the CSP understands and authorizes the legal and privacy boundaries of this type of analysis, obtaining such data may enable a company to identify at-risk individuals, potentially enabling an intervention before an attack is realized.

Monitoring- and auditing-related data for a SIEM system could provide foundational elements to support such analyses. A proposed model that may enable a similar approach is discussed in the paper *Proactive Insider Threat Detection through Graph Learning and Psychological Context* [Brdiczka 2012].

5.1.3 End-User Awareness: Insider Threat Training Vignettes

Modularized security-awareness training vignettes that describe specific insider threat considerations may help CSPs to communicate and emphasize the risk that insiders pose to their daily operations and mission fulfillment.

Conveying various insider scenarios to employees via direct, web-based, mobile-capable videos that integrate with corporate learning management systems can help CSPs to address weaknesses in awareness and training while meeting annual compliance objectives. The *Securing the Human* program developed by the SANS Institute [SANS 2013] is an example of such training.

5.1.4 User-Profiling Tools

There is an overabundance of diagnostic sensor data from log files, syslog services, network flow records, packet capture, and other sources. However, to manage the IaaS, PaaS, and SaaS cloud framework, CSPs must also create a set of tools with supporting middleware that can be used to begin profiling specific high-profile users and their actions in the control plane. While new practices and methods need to be developed, simple statistical and production rule methods can go a long way in providing alert and discovery mechanisms as well as a forensic platform for insider threat vectors.

6 Limitations of Our Analysis

This preliminary analysis is designed to provide DHS with a general sense of how CSPs may be currently addressing insider threat practices through administrative and technical controls. We acknowledge the limitations of this analysis, including but not limited to the following areas:

- inquiry-based observations—The observations described in this report were obtained through inquiry alone, during 60- to 90-minute interviews with CSP personnel. We did not validate participants' responses regarding their CSPs' operations against the administrative or technical controls that were actually implemented, and we assumed that each single respondent represented her or his entire CSP. Additionally, we did not verify CSP compliance with and/or accreditation for a specific security model.
- limited CSP respondents—While we contacted a number of CSPs for this analysis, only a few agreed to speak with us regarding their current insider threat management programs and processes. We assured all potential participants that we would treat all obtained data as controlled information (CI) per the SEI's Code of Business and Ethics and Compliance. Regardless, those who did not participate said they would still want to execute a nondisclosure agreement. Another CSP expressed concerns regarding discoverability and the Freedom of Information Act (FOIA), which we unsuccessfully tried to allay.
- interview duration versus breadth of subject matter—Our interviews were limited by time constraints; appropriate CSP personnel were able to provide, on average, only 70 minutes of their time to speak with us regarding their current insider threat management practices. This constraint clearly affected the number of data points we could obtain. Despite the limited breadth of insider threat topics covered during interviews, indicators regarding common practices did emerge. In many ways, this analysis merely scratches the surface of CSPs' existing processes for managing insider threat.

7 Conclusion

Within the information security programs of the CSPs that participated in this analysis, the implementation of insider threat management techniques as recognized practices appears to be emerging and developing. While technical controls are in place to help detect malicious insider activities, the underlying business processes that support effective detection and mitigation in CSPs are generally unstructured. We made similar observations regarding administrative controls as well, particularly in connection with formal security awareness and training regarding insider attacks.

The CSP sector is like others that are attempting to address similar concerns attributable to insider events, such as the theft of intellectual property and sensitive data. These threats continue to challenge other verticals, such as health care, manufacturing, finance, and technology. Given the enormous growth of the CSP sector, its members' priorities are market expansion, customer acquisition, and service differentiation. At present, it appears that the insider threat vector has not yet become a priority in the majority of the CSP sector.

Organizations can mitigate insider attacks by using a layered, comprehensive strategy consisting of risk-based administrative, physical, and technical controls. Data indicating current insider threat management countermeasures are limited at best, so aiding cloud security research efforts such as this one makes a meaningful contribution to the CSP community as a whole. Understanding common issues, such as what is working and what is not, may elicit additional considerations and spur further development of security management processes that can be used to reduce the risks of insider attacks.

The participating CSPs' voluntary engagement in this project strongly indicates that they are interested in improving their existing insider threat management capabilities and seeking useful input and process guidance from trusted sources, such as the research and analysis provided by the CERT Insider Threat Center. The next phase of this project will continue to extend interview requests and may help us determine better methods for increasing the number of CSP participants.

References

URLs are valid as of the publication date of this document.

[Brdiczka 2012]
Brdiczka, Oliver; Liu, Juan; Price, Bob; Shen, Jianqiang; Patil, Akshay; Chow, Richard; Bart, Eugene; & Ducheneaut, Nicholas. *Proactive Insider Threat Detection through Graph Learning and Psychological Context*. Palo Alto Research Center (PARC), 2012. http://www.parc.com/content/attachments/proactive-insider-threat-detection.pdf

[Cappelli 2012]
Cappelli, Dawn; Moore, Andrew; & Trzeciak, Randall. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley Professional, 2012. http://www.sei.cmu.edu/library/abstracts/books/9780321812575.cfm

[CERT Insider Threat Center 2011]
CERT Insider Threat Center. *Insider Threat Control: Using a SIEM Signature to Detect Potential Precursors to IT Sabotage.* Software Engineering Institute, Carnegie Mellon University, 2011. http://www.cert.org/archive/pdf/SIEM-Control.pdf

[CSA 2013]
Cloud Security Alliance. *The Notorious Nine: Cloud Computing Top Threats in 2013*. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/ (2013).

[GSA 2013]
U.S. General Services Administration. *Federal Risk and Authorization Management Program (FedRAMP)*. http://fedramp.gov (2013).

[ISO/IEC 2005]
International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *ISO/IEC 27001:2005, Information Technology—Security Techniques—Information Security Management Systems—Requirements*. British Standards Institution, 2005. http://bsi.learncentral.com/shop/Course.aspx?id=12772&name=BS+ISO%2fIEC+27001%3a2005

[Mell 2011]
Mell, Peter & Grance, Timothy. *The NIST Definition of Cloud Computing (NIST Special Publication 800-145)*. National Institute of Standards and Technology (NIST), 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[Mello 2013]
Mello, John P. “Assess Risk Before You Ascend to the Cloud.” *CSO Online*. http://www.csoonline.com/article/732276/assess-risk-before-you-ascend-to-the-cloud (2013).

[NIST 2009]
National Institute of Standards and Technology (NIST): Computer Security Division Information Technology Laboratory. *Recommended Security Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53, Revision 3).* NIST, 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[NIST 2013]
National Institute of Standards and Technology (NIST): Computer Security Division Information Technology Laboratory. *Module Validation Lists.* http://csrc.nist.gov/groups/STM/cmvp/validation.html (2013).

[Ponemon 2012]
Ponemon Institute. *2012 Cost of Cyber Crime Study: United States*. Ponemon Institute, 2012. http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

[SANS 2013]
SANS Institute. *Securing the Human: Insider Threat.* http://www.securingthehuman.org/enduser/enduser-videos/insider-threat (2013).

[Silowash 2012]
Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017

[Verizon 2013]
Verizon. *2013 Data Breach Investigations Report.* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (2013).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	November 2013	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase I	FA8721-05-C-0003

6. AUTHOR(S)

Greg Porter

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

CMU/SEI-2013-TN-020

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFLCMC/PZE/Hanscom
Enterprise Acquisition Division
20 Schilling Circle
Building 1305
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

In early 2013, researchers in the CERT® Insider Threat Center contacted commercial and government cloud service providers (CSPs) about participating in research to gain a preliminary understanding of implemented administrative and technical controls that they are using to identify and manage the threats posed by insiders. These CSP participants provided frank and meaningful insight about their insider threat management programs and enterprise security practices. This report contains the observations obtained from interviewing the CSP personnel who volunteered to participate as well as an analysis of CSP management of insider threat based on the information obtained in interviews, observations of implemented insider threat controls, and risk considerations.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Insider threat; cloud service providers	29

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL